

In the claims

Cancel claims 1-15, 17- 28, and 30-56 without prejudice or disclaimer.

1 16. (Once Amended) A system for maintaining security in a distributed computing
2 environment, comprising:
3 a policy manager for managing a security policy; and
4 an application guard for managing access to securable components as specified by
5 the security policy;

6 [The system of claim 1,] wherein the application guard further allows for
7 additional customized code to process and evaluate authorization requests
8 based on the additional customized code.

1 29. (Once Amended) A system for controlling user access in a distributed computing
2 environment, comprising:
3 a global policy specifying access privileges of the user to securable components;
4 a policy manager located on a server for managing and distributing a local client
5 policy based on the global policy to a client, and
6 an application guard located on the client for managing access to the securable
7 components as specified by the local client policy;

8 [The system of claim 18,] wherein the application guard further allows for
9 additional customized code to process and evaluate authorization requests
10 based on the additional customized code.

RECEIVED
MAY 1 - 2001
Technology Center 2100

Add new claims 57-89

1 57. A system for maintaining security in a distributed computing environment,
2 comprising:
3 a policy manager for managing a security policy; and
4 an application guard for managing access to securable components including at
5 least one application as specified by the security policy.

1 58. A system for maintaining security in a distributed computing environment,
2 comprising:
3 a policy manager for managing a security policy; and
4 an application guard for managing access to securable components including a
5 function within an application as specified by the security policy.

1 59. A system for maintaining security in a distributed computing environment,
2 comprising:
3 a policy manager for managing a security policy; and
4 an application guard for managing access to securable components including a
5 procedure within an application as specified by the security policy.

1 60. A system for maintaining security in a distributed computing environment,
2 comprising:
3 a policy manager for managing a security policy; and
4 an application guard for managing access to securable components including a
5 data structure within an application as specified by the security policy.

1 61. A system for maintaining security in a distributed computing environment,
2 comprising:
3 a policy manager for managing a security policy; and
4 an application guard for managing access to securable components including a
5 database object referenced by an application as specified by the security
6 policy.

1 62. A system for maintaining security in a distributed computing environment,
2 comprising:
3 a policy manager for managing a security policy; and
4 an application guard for managing access to securable components including a
5 file system object referenced by an application as specified by the security
6 policy.

1

1 63. A method for maintaining security in a distributed computing environment,
2 comprising:
3 managing a security policy via a policy manager; and
4 managing access via an application guard to securable components including at
5 least one application as specified by the security policy.

1 64. A method for maintaining security in a distributed computing environment,
2 comprising:
3 managing a security policy via a policy manager; and
4 managing access via an application guard to securable components including a
5 function within an application as specified by the security policy.

1 65. A method for maintaining security in a distributed computing environment,
2 comprising:
3 managing a security policy via a policy manager; and
4 managing access via an application guard to securable components including a
5 procedure within an application as specified by the security policy.

1 66. A method for maintaining security in a distributed computing environment,
2 comprising:
3 managing a security policy via a policy manager; and
4 managing access via an application guard to securable components including a
5 data structure within an application as specified by the security policy.

1 67. A method for maintaining security in a distributed computing environment,
2 comprising:
3 managing a security policy via a policy manager; and
4 managing access via an application guard to securable components including a
5 database object referenced by an application as specified by the security
6 policy.

1 68. A method for maintaining security in a distributed computing environment,
2 comprising:
3 managing a security policy via a policy manager; and
4 managing access via an application guard to securable components including a
5 file system object referenced by an application as specified by the security
6 policy.

1 69. A method for maintaining security in a distributed computing environment,
2 comprising:
3 managing a security policy via a policy manager; and
4 managing via an application guard access to securable components as specified by
5 the security policy;
6 wherein the application guard further allows for additional customized code to
7 process and evaluate authorization requests based on the additional
8 customized code.

1 70. A method for controlling user access via a system in a distributed computing
2 environment, comprising:
3 specifying access privileges of the user via a global policy to securable
4 components;
5 managing and distributing via a policy manager a local client policy based on the
6 global policy located on a server to a client, and
7 managing access via an application guard located on the client to the securable
8 components as specified by the local client policy;
9 wherein the application guard further allows for additional customized code to
10 process and evaluate authorization requests based on the additional
11 customized code.

1 71. A method for authorization that provides access to securable components of a
2 system for a user, comprising:
3 specifying access privileges of the user via a policy to the securable components
4 managing access via an application guard to the securable components; and
5 executing via a processor coupled to said system said application guard;
6 wherein the application guard further allows for additional customized code to
7 process and evaluate authorization requests based on the additional
8 customized code.

1 72. A method for providing a system for maintaining security in a distributed
2 computing environment, comprising:
3 providing a policy manager for managing a security policy; and
4 providing an application guard for managing access to securable components
5 including at least one application as specified by the security policy.

1 73. A method for providing a system for maintaining security in a distributed
2 computing environment, comprising:
3 providing a policy manager for managing a security policy; and
4 providing an application guard for managing access to securable components
5 including a function within an application as specified by the security
6 policy.

1 74. A method for providing a system for maintaining security in a distributed
2 computing environment, comprising:
3 providing a policy manager for managing a security policy; and
4 providing an application guard for managing access to securable components
5 including a procedure within an application as specified by the security
6 policy.

1 75. A method for providing a system for maintaining security in a distributed
2 computing environment, comprising:
3 providing a policy manager for managing a security policy; and
4 providing an application guard for managing access to securable components
5 including a data structure within an application as specified by the security
6 policy.

1 76. A method for providing a system for maintaining security in a distributed
2 computing environment, comprising:
3 providing a policy manager for managing a security policy; and
4 providing an application guard for managing access to securable components
5 including a database object referenced by an application as specified by
6 the security policy.

1 77. A method for providing a system for maintaining security in a distributed
2 computing environment, comprising:
3 providing a policy manager for managing a security policy; and
4 providing an application guard for managing access to securable components
5 including a file system object referenced by an application as specified by
6 the security policy.

1 78. A method for providing a system for maintaining security in a distributed
2 computing environment, comprising:
3 providing a policy manager for managing a security policy; and
4 providing an application guard for managing access to securable components as
5 specified by the security policy;
6 wherein the application guard further allows for additional customized code to
7 process and evaluate authorization requests based on the additional
8 customized code.

1 79. A method for providing a system for controlling user access in a distributed
2 computing environment, comprising:
3 providing a global policy specifying access privileges of the user to securable
4 components;
5 providing a policy manager located on a server for managing and distributing a
6 local client policy based on the global policy to a client, and
7 providing an application guard located on the client for managing access to the
8 securable components as specified by the local client policy;
9 wherein the application guard further allows for additional customized code to
10 process and evaluate authorization requests based on the additional
11 customized code.

1 80. A method for providing a system for authorization that provides access to
2 securable components for a user, comprising:
3 providing a policy specifying access privileges of the user to the securable
4 components;
5 providing an application guard; and
6 providing a processor coupled to said system, said processor executing said
7 application guard to manage access to the securable components;
8 wherein the application guard further allows for additional customized code to
9 process and evaluate authorization requests based on the additional
10 customized code.

1 81. A computer readable storage medium having stored thereon a method for
2 maintaining security in a distributed computing environment comprising the steps of:
3 managing a security policy via a policy manager; and
4 managing access via an application guard to securable components including at
5 least one application as specified by the security policy.

1 82. A computer readable storage medium having stored thereon a method for
2 maintaining security in a distributed computing environment comprising the steps of:
3 managing a security policy via a policy manager; and
4 managing access via an application guard to securable components including a
5 function within an application as specified by the security policy.

1 83. A computer readable storage medium having stored thereon a method for
2 maintaining security in a distributed computing environment comprising the steps of:
3 managing a security policy via a policy manager; and
4 managing access via an application guard to securable components including a
5 procedure within an application as specified by the security policy.

1 84. A computer readable storage medium having stored thereon a method for
2 maintaining security in a distributed computing environment comprising the steps of:
3 managing a security policy via a policy manager; and
4 managing access via an application guard to securable components including a
5 data structure within an application as specified by the security policy.

1 85. A computer readable storage medium having stored thereon a method for
2 maintaining security in a distributed computing environment comprising the steps of:
3 managing a security policy via a policy manager; and
4 managing access via an application guard to securable components including a
5 database object referenced by an application as specified by the security
6 policy.

1 86. A computer readable storage medium having stored thereon a method for
2 maintaining security in a distributed computing environment, comprising:
3 managing a security policy via a policy manager; and
4 managing access via an application guard to securable components including a
5 file system object referenced by an application as specified by the security
6 policy.

1 87. A computer readable storage medium having stored thereon a method for
2 maintaining security in a distributed computing environment comprising the steps of:
3 managing a security policy via a policy manager; and
4 managing via an application guard access to securable components as specified by
5 the security policy;
6 wherein the application guard further allows for additional customized code to
7 process and evaluate authorization requests based on the additional
8 customized code.

1 88. A computer readable storage medium having stored thereon a method for
2 controlling user access via a system in a distributed computing environment, comprising
3 the steps of:

4 specifying access privileges of the user via a global policy to securable

5 components;

6 managing and distributing via a policy manager a local client policy based on the

7 global policy located on a server to a client, and

8 managing access via an application guard located on the client to the securable

9 components as specified by the local client policy;

10 wherein the application guard further allows for additional customized code to

11 process and evaluate authorization requests based on the additional

12 customized code.

1 89. A computer readable storage medium having stored thereon a method for
2 authorization that provides access to securable components of a system for a user,
3 comprising:

4 specifying access privileges of the user via a policy to the securable components

5 managing access via an application guard to the securable components; and

6 executing via a processor coupled to said system said application guard;

7 wherein the application guard further allows for additional customized code to

8 process and evaluate authorization requests based on the additional

9 customized code.